DESIGNATED PLACE FRAMEWORK

Operational Geography for P-Series Instruments

January 2022

Dr. F. Patterson

Standards Working Group · Standard Index Group
1 Lombard Street
London EC3V 9AA
United Kingdom

ABSTRACT

The Designated Place (DP) framework establishes standardized location topology for secure storage of sensitive estate information. This technical note defines the DP-xx coding convention, access protocols, and physical/digital custody arrangements. Problem Statement: Traditional estate documentation conflates three distinct concepts:

1. The inventory (what exists)
2. The secrets (credentials, keys, combinations)
3. The location (where secrets are stored)

This conflation creates security vulnerability. If the inventory document is compromised, all secrets are exposed. Solution: The DP framework separates these layers:

- P-Series instruments = inventory (public-safe)
- DP-xx locations = custody points (referenced, not detailed)
- DP contents = actual secrets (physically/digitally secured)

This separation maintains security while preserving continuity. Scope: This note covers:

- DP coding conventions
- Physical custody protocols
- Digital custody protocols
- Hybrid arrangements
- Access control standards
- Registry requirements

DP CODING CONVENTION

Format: DP-XX (where XX = sequential number, zero-padded) Examples:

- DP-01 (first designated place)
- DP-02 (second designated place)
- DP-15 (fifteenth designated place)

Rules:

1. Sequential numbering - DP codes assigned in order of establishment
2. Zero-padded - Always two digits (DP-01, not DP-1)
3. Hyphenated - Always DP-01 (not DP01 or DP.01)
4. Permanent - Once assigned, DP codes never change
5. Non-hierarchical - DP-01 is not "more important" than DP-15

Common Allocations:

- DP-01: Primary password vault (digital)
- DP-02: Fire-rated home safe (physical)
- DP-03: Bank safety deposit box (physical)
- DP-04: Encrypted cloud backup (digital)
- DP-05: Executor's sealed packet (physical)
- DP-06: Solicitor's custody (physical)
- DP-07: Secondary password vault (digital backup)

Registry Requirement: All DP codes must be documented in the R-04: Designated Place Registry with:

- DP code
- Location type (physical/digital/hybrid)
- Access protocol
- Custodian (if applicable)
- Cross-references to P-Series instruments

PHYSICAL CUSTODY PROTOCOLS

Definition: Physical DP = tangible location where documents/keys/objects are stored
Common Physical DPs:

DP Type: Home Safe

Specifications:

- Fire rating: Minimum 1-hour @ 1700°F
- Burglary rating: TL-15 or better recommended
- Size: Adequate for letter-size documents + objects
- Location: Secured to structure (bolted/embedded)

Access Protocol:

- Combination or key-based
- Documented in R-04 (DP Registry)
- Combination NOT written in P-Series instruments
- Recovery mechanism established (backup combination stored in different DP)

Contents Typical:

- Original wills, trusts, POAs
- Property deeds
- Insurance policies
- Jewelry, precious items
- USB drives (encrypted backups)
- Physical keys

DP Type: Bank Safety Deposit Box

Specifications:

- Bank: Established institution (avoid boutique banks)
- Box size: Medium to large
- Co-access: Consider joint access with executor
- Annual fee: Prepaid or automated payment

Access Protocol:

- Physical key + bank identification
- Bank hours constraint (M-F 9-5 typical)
- Multiple signatories possible
- Estate access procedures documented

Contents Typical:

- Original certificates (birth, marriage, death of predecessors)
- Share certificates, bonds (if physical)
- Collectibles, small valuables
- Backup USB drives

- Secondary executor packet

Risks:

- Bank failure (rare but possible)
- Access delays during bank hours
- Executor may face access challenges post-death

Mitigation:

- Duplicate critical documents in DP-02 (home safe)
- Establish co-access with trusted executor
- Annual verification protocol

DP Type: Solicitor/Advisor Custody

Specifications:

- Established firm (10+ years operation)
- Professional indemnity insurance
- Conflict check (no conflicting client interests)
- Fee structure transparent

Access Protocol:

- Sealed packet arrangement
- Conditional release (upon death, incapacity)
- Dual control (solicitor + executor notification)

Contents Typical:

- Executor letter of wishes
- Distribution instructions
- Sensitive family information
- Backup encryption keys

DIGITAL CUSTODY PROTOCOLS

Definition: Digital DP = electronic storage where credentials/files are secured Common Digital DPs:

DP Type: Password Manager

Approved Technologies:

- 1Password (recommended - family/team plans)
- Bitwarden (recommended - self-hosted option)
- KeePass (recommended - local-only option)

NOT Approved:

- Browser password managers (fragile)
- Unencrypted spreadsheets
- Plain text files
- Cloud notes without encryption

Configuration:

- Master password: Strong (20+ characters, mixed case, symbols)
- Two-factor: Hardware key (YubiKey) preferred over SMS
- Recovery: Emergency kit stored in physical DP
- Backup: Encrypted vault file stored in multiple physical DPs

Contents Typical:

- All online account credentials
- WiFi passwords
- Safe combinations (cross-reference to physical DP)
- Security question answers
- Recovery codes

Access Protocol:

- Master password known to principal
- Emergency kit with recovery details in DP-02 (home safe)
- Executor provided master password post-event
- Family account option (shared vault for spouse)

DP Type: Encrypted Cloud Storage

Approved Technologies:

- Tresorit (zero-knowledge encryption)
- SpiderOak (zero-knowledge encryption)
- Cryptomator + any cloud provider (DIY encryption)

NOT Approved:

- Unencrypted Dropbox/Google Drive/iCloud
- Services without zero-knowledge encryption

- Free-tier accounts (risk of deletion)

Configuration:

- Client-side encryption (provider cannot decrypt)
- Local encryption key stored in password manager (DP-01)
- Multi-device sync
- Version history enabled
- 2FA required

Contents Typical:

- Encrypted backups of P-Series instruments
- Scanned documents (passport, insurance, deeds)
- Financial statements
- Medical records
- Family photos (archival)

Access Protocol:

- Encryption key in password manager (DP-01)
- Executor provided password manager access
- Recovery account credentials in executor packet (DP-05)

DP Type: Encrypted USB Drives

Specifications:

- Hardware encryption (Apricorn, Kingston IronKey)
- USB 3.0 or better
- Minimum 32GB capacity
- PIN-based unlock

Configuration:

- PIN: 8-12 digits
- PIN documented in DP-01 (password manager)
- Duplicate drives (primary + backup)
- Stored in separate physical locations

Contents Typical:

- Complete P-Series instrument set (encrypted PDF)
- Password manager vault backup
- Critical documents bundle
- Recovery instructions

Storage:

- Primary: DP-02 (home safe)
- Backup: DP-03 (bank deposit box)

HYBRID ARRANGEMENTS

Definition: Hybrid DP = combination of physical and digital custody Example 1: Physical Safe + Digital Key

```
DP-02: Home Safe (Physical)
▯▯▯ Physical contents: Documents, jewelry
▯▯▯ Combination stored in: DP-01 (Password Manager)
```

Advantage: Physical security + digital convenience Risk: Requires access to both DPs

---

Example 2: Cloud Storage + Physical Recovery Key

```
DP-04: Encrypted Cloud Storage (Digital)
▯▯▯ Digital contents: Scanned documents, backups
▯▯▯ Encryption key stored in: DP-02 (Home Safe, USB drive)
```

Advantage: Cloud accessibility + offline recovery Risk: Physical DP compromise exposes digital DP

Example 3: Password Manager + Physical Emergency Kit

```
DP-01: 1Password (Digital)
▯▯▯ Digital contents: All credentials
▯▯▯ Emergency Kit stored in: DP-02 (Home Safe, printed)
```

Advantage: Secure primary + accessible backup Risk: Printed emergency kit must be updated

---

ACCESS CONTROL STANDARDS

Principle: Minimize access points while maintaining executor continuity Access Tiers:

Tier 1: Principal Only

- Full access to all DPs
- Master passwords, combinations, keys
- Authority to modify/restructure

Tier 2: Spouse/Partner (Optional)

- Shared access to specific DPs (joint accounts)
- Independent access to personal DPs
- Family vault in password manager

Tier 3: Executor (Conditional)

- NO access during principal's lifetime
- Conditional access upon death/incapacity trigger
- Sealed packets, escrow arrangements
- Executor letter provides DP locations + access methods

Tier 4: Professional Advisors (Limited)

- Access to specific information only
- No credential access
- Information via P-Series instruments (pointers, not secrets)
- Professional custody (solicitor holds sealed packet)

Golden Rule: The P-Series instruments can be shared safely. DP access details cannot.

DP TOPOLOGY DIAGRAM

DIN INDUSTRIAL DIAGRAM: DP HIERARCHY

```
DESIGNATED PLACE TOPOLOGY
┌─────────────────────────────────────────────────────────┐
│ P-SERIES INSTRUMENTS (Public-Safe Layer) │
│ [P-01 through P-10] │
│ • References DP codes │
│ • Contains NO secrets │
└─────────────────────────────────────────────────────────┘
│
│ points to
│
┌─────────────────────────────────────────────────────────┐
│ R-04: DP REGISTRY (Index Layer) │
│ • Lists all DP codes │
│ • Location types │
│ • Access protocols (generic) │
└─────────────────────────────────────────────────────────┘
│
│ describes
│
┌──────────────────────────────────────────────────────────────────────┐
│ DESIGNATED PLACES (Custody Layer) │
│ │
│ ┌──────────────┐ ┌──────────────┐ ┌──────────────┐ ┌──────────────┐ │
│ │ DP-01 │ │ DP-02 │ │ DP-03 │ │ DP-04 │ │
│ │ PASSWORD │ │ HOME │ │ BANK │ │ CLOUD │ │
│ │ MANAGER │ │ SAFE │ │ DEPOSIT │ │ STORAGE │ │
│ │ (DIGITAL)│ │(PHYSICAL)│ │(PHYSICAL)│ │(DIGITAL)│ │
│ └──────────────┘ └──────────────┘ └──────────────┘ └──────────────┘ │
│ │
└──────────────────────────────────────────────────────────────────────┘
│
│ contains
│
┌─────────────────────────────────────────────────────────┐
│ ACTUAL SECRETS (Content Layer) │
│ • Passwords, keys, combinations │
│ • Original documents │
│ • Credentials, access codes │
└─────────────────────────────────────────────────────────┘
SECURITY POSTURE:
- Compromise of P-Series: No secrets exposed
- Compromise of R-04: Location types known, not contents
- Compromise of single DP: Limited exposure
- Full estate access: Requires P-Series + R-04 + DP access
```

REGISTRY REQUIREMENTS

(R-04) Mandatory Fields for Each DP:

```
R-04: DESIGNATED PLACE REGISTRY
▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒
▒ DP-01: Password Manager (1Password) ▒
▒ Type: Digital ▒
▒ Location: Cloud + Local Backup ▒
▒ Access: Master password + YubiKey ▒
▒ Custodian: Principal ▒
▒ Recovery: Emergency kit in DP-02 ▒
▒ Referenced by: P-01, P-02, P-03, P-06, P-07, P-09 ▒
▒ Last verified: 2024-08-15 ▒
▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒
```

Annual Review Protocol:

- Verify all DP locations still exist
- Test access methods
- Update access credentials if changed
- Confirm recovery mechanisms functional
- Document verification in R-04

IMPLEMENTATION NOTES

Starting Configuration (Minimum Viable):

- DP-01: Password manager (1Password or Bitwarden)
- DP-02: Fire-rated home safe
- DP-03: Bank safety deposit box (optional, recommended for £100k+ estates)

Scaling:

- £5M-£50M estates: 3-5 DPs typical
- £50M-£500M estates: 5-8 DPs typical
- Multi-jurisdiction estates: +2 DPs per jurisdiction

Common Mistakes:

- ☒ Too many DPs (creates complexity)
- ☒ Circular dependencies (DP-01 key in DP-02, DP-02 combination in DP-01)
- ☒ Single point of failure (all keys in one DP)
- ☒ Unrecoverable access (master password known only to deceased)

Best Practices:

- ☑ Redundancy (critical items duplicated across 2 DPs)
- ☑ Independent recovery (each DP recoverable without others)
- ☑ Executor access path (clear instructions in sealed packet)
- ☑ Annual verification (test access, update registry)

External Reference: ISO 27001:2013 - Information security management systems. The DP framework implements physical and digital custody controls consistent with ISO 27001 Annex A.11 (Physical and environmental security) and A.12 (Operations security).

FOOTER:

`TN-01: Designated Place Framework v1.0 | Page X of 10 | Standard Index Group | Technical Note`

END TN-01